PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 9.4.2001

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T

Hakija
Applicant

Sonera Oyj
Helsinki, FI

Kansainvälinen patenttihakemus nro **PCT/FI99/00851**
International patent application no

Kansainvälinen tekemispäivä **14.10.1999**
International filing date

Etuoikeushak. nro **FI 982232**
Priority from appl.

Tekemispäivä **14.10.1998**
Filing date

Keksinnön nimitys
Title of invention

"Method and system for the applicaton of a safety marking"

Hakemus on siirtynyt **Sonera Smarttrust Oy**:lle.
The application has been assigned to **Sonera Smarttrust Oy.**

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä kansainvälisiä patenttihakemuksia vastaanottavana viranomaisena toimivalle Patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista sekä niihin tehdyistä korjauksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawing, originally filed with the Finnish Patent Office acting as receiving Office for the international patent applications, and of any corrections thereto.

Pirjo Kaila
Tutkimussihteeri

Maksu 300,- mk
Fee 300,- FIM

Osoite: Arkadiankatu 6 A
Address: P.O.Box 1160
FIN-00101 Helsinki, FINLAND

Puhelin: 09 6939 500
Telephone: + 358 9 6939 500

Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

HOME COPY

PCT REQUEST

12463S

Original (for **SUBMISSION**) - printed on 14.10.1999 02:30:42 PM

0	**For receiving Office use only**	
0-1	International Application No.	PCT/FI 9 9 / 0 0 8 5 1
0-2	International Filing Date	1 4 OCT 1999 (1 4. 10. 99)
0-3	Name of receiving Office and "PCT International Application"	The Finnish Patent Office PCT International Application
0-4	**Form - PCT/RO/101 PCT Request**	
0-4-1	Prepared using	PCT-EASY Version 2.84 (updated 01.07.1999)
0-5	**Petition** The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	**Receiving Office (specified by the applicant)**	National Board of Patents and Registration (Finland) (RO/FI)
0-7	**Applicant's or agent's file reference**	12463S
I	**Title of invention**	METHOD AND SYSTEM FOR THE APPLICATION OF A SAFETY MARKING
II	**Applicant**	
II-1	This person is:	applicant only
II-2	Applicant for	all designated States except US
II-4	Name	SONERA OYJ
II-5	Address:	Teollisuuskatu 15 FIN-00510 HELSINKI Finland
II-6	State of nationality	FI
II-7	State of residence	FI
III-1	**Applicant and/or inventor**	
III-1-1	This person is:	applicant and inventor
III-1-2	Applicant for	US only
III-1-4	Name (LAST, First)	VATANEN, Harri
III-1-5	Address:	40 Alma Road Windsor, SL4 3HJ Berkshire United Kingdom
III-1-6	State of nationality	FI
III-1-7	State of residence	GB

RO/FI

PCT REQUEST

12463S

Original (for **SUBMISSION**) - printed on 14.10.1999 02:30:42 PM

IV-1	**Agent or common representative; or address for correspondence** The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	agent
IV-1-1	Name	PAPULA REIN LAHTELA OY
IV-1-2	Address:	P.O. Box 981 (Fredrikinkatu 61 A) FIN-00101 HELSINKI Finland
IV-1-3	Telephone No.	+358 9 3480 060
IV-1-4	Facsimile No.	+358 9 3480 0630
IV-1-5	e-mail	papula@papula.fi
V	**Designation of States**	
V-1	Regional Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AP: GH GM KE LS MW SD SL SZ UG ZW and any other State which is a Contracting State of the Harare Protocol and of the PCT EA: AM AZ BY KG KZ MD RU TJ TM and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE and any other State which is a Contracting State of the European Patent Convention and of the PCT OA: BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG and any other State which is a member State of OAPI and a Contracting State of the PCT
V-2	National Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AE AL AM AT AU AZ BA BB BG BR BY CA CH&LI CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
V-3	National Patent (States which have become party to the PCT after the issuance of this version of EASY)	MA

PCT REQUEST

12463S

Original (for **SUBMISSION**) - printed on 14.10.1999 02:30:42 PM

V-5	**Precautionary Designation Statement** In addition to the designations made under items V-1, V-2 and V-3, the applicant also makes under Rule 4.9(b) all designations which would be permitted under the PCT except any designation(s) of the State(s) indicated under item V-6 below. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit.		
V-6	**Exclusion(s) from precautionary designations**	NONE	
VI-1	**Priority claim of earlier national application**		
VI-1-1	Filing date	14 October 1998 (14.10.1998)	
VI-1-2	Number	982232	
VI-1-3	Country	FI	
VII-1	**International Searching Authority Chosen**	Swedish Patent Office (ISA/SE)	
VIII	**Check list**	number of sheets	electronic file(s) attached
VIII-1	Request	4	-
VIII-2	Description	10	-
VIII-3	Claims	3	-
VIII-4	Abstract	1	12463s.txt
VIII-5	Drawings	2	-
VIII-7	TOTAL	20	
	Accompanying items	paper document(s) attached	electronic file(s) attached
VIII-8	Fee calculation sheet	✓	-
VIII-16	PCT-EASY diskette	-	diskette
VIII-18	**Figure of the drawings which should accompany the abstract**	1	
VIII-19	**Language of filing of the international application**	Finnish	
IX-1	**Signature of applicant or agent**		
IX-1-1	Name	PAPULA REIN LAHTELA OY	
IX-1-2	Name of signatory	Timo Helino	

FOR RECEIVING OFFICE USE ONLY

10-1	**Date of actual receipt of the purported international application**	14 OCT 1999	(14-10-1999)
10-2	**Drawings:**		
10-2-1	Received		
10-2-2	Not received		

PCT REQUEST

12463S

Original (for **SUBMISSION**) - printed on 14.10.1999 02:30:42 PM

10-3	Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application	
10-4	Date of timely receipt of the required corrections under PCT Article 11(2)	
10-5	International Searching Authority	ISA/SE
10-6	Transmittal of search copy delayed until search fee is paid	

FOR INTERNATIONAL BUREAU USE ONLY

11-1	Date of receipt of the record copy by the International Bureau	

MENETELMÄ JA JÄRJESTELMÄ TURVAMERKINNÄN KÄYTTÄMISEKSI

KEKSINNÖN ALA

Esillä oleva keksintö koskee elektronista turvamerkintää. Erityisesti esillä olevan keksinnön kohteena on uusi ja parannettu menetelmä ja järjestelmä sähköisessä muodossa olevan turvamerkinnän käyttämiseksi esineiden ja laitteiden merkitsemiseen.

TEKNIIKAN TASO

Turvamerkintää käytetään esineiden, laitteiden sekä informaation merkintään niiden suojaamiseksi varkaudelta ja väärinkäytöltä. Turvamerkintä voi olla laitteeseen kaiverrettu omistajan sosiaaliturvatunnus, nimi tai muu tieto, joka yksilöi laitteen omistajan. Tämän toteuttaminen on kuitenkin hankalaa, koska kaivertaminen tai muu vastaava fyysinen merkintätapa voi aiheuttaa merkittävälle laitteelle vaurioita ja merkintä on usein epäesteettinen.

Turvamerkintä voi perustua myös biometriseen tietoon, jollainen on esimerkiksi DNA, sormenjälki tai silmästä saatava tieto, jolloin henkilön identiteetti on paremmin varmistettavissa. Toisaalta esimerkiksi kloonatuilla yksilöillä DNA on identtinen, mutta sormenjälki erilainen. Tunnistuksen tarkkuutta voidaan entisestään parantaa yhdistämällä erilaisia toisistaan riippumattomia tunnisteita. Ihmisen DNA voidaan muodostaa $2^{44} \approx 1{,}76 * 10^{13}$ erilaisella tavalla. Vastaavasti maapallon väkiluvun suuruusluokka on noin 10^{10}. Yhdistämällä DNA:han siitä riippumaton sormenjälki, ja esimerkiksi matkaviestimen yhteydessä esiintyvä PIN-koodi saadaan erilaisiksi kombinaatioiksi esimerkiksi 10^{29}.

Nykyään esineitä voidaan merkitä myös sähköisellä tai elektronisella turvamerkinnällä, jonka perusideana on merkitä esineet pienellä koodatulla tur-

vasirulla, jonka sisältämän merkintätiedon voi lukea ja tunnistaa ainoastaan erikoislukulaitteilla. Eräs tällainen järjestelmä perustuu transponderitekniikkaan, joka on liitetty lähes näkymättömiin siruihin. Yleensä sirut ovat passiivisia, jolloin niitä ei voida uudelleen ohjelmoida, mikä estää niiden väärentämisen ja ne eivät myöskään näin ollen ole herkkiä sähkömagneettiselle säteilylle. Elektronista turvamerkintää käytetään siten, että asiakas ostaa turvamerkinnän valtuutetulta jälleenmyyjältä. Jälleenmyyjä asentaa mikrosirun merkittävään esineeseen, minkä jälkeen rekisterikortin avulla rekisteröidään merkintä kolmannen osapuolen ylläpitämään tietokantaan.

Kun varastettu ja turvamerkitty esine löydetään, luetaan erikoislukulaitteella sirun sisältämä sähköinen informaatio. Tätä informaatiota verrataan kolmannen osapuolen tietokantaan, jolloin tietokannasta saadaan selville esineen oikea omistaja. Tällainen järjestely kuitenkin vaatii erityisen rekisteröintitietokannan, joka vaatii ylläpitoa ja on siten hankala käyttää. Lisäksi lukulaitetta tai luettua informaatiota voidaan muokata tai manipuloida ennen rekisteritietokannasta tehtävää kyselyä. Tämän johdosta järjestelmään ei voi täysin luottaa.

Esillä olevan keksinnön tarkoituksena on poistaa edellä esitetyt ongelmat.

Erityisesti esillä olevan keksinnön tarkoituksena on tuoda esiin uudentyyppinen menetelmä ja järjestelmä esineiden, laitteiden tai informaation elektronista merkintää varten. Keksinnön tarkoituksena on yksinkertaistaa merkittyjen laitteiden tunnistaminen ja aikaansaada järjestelmä, joka on ehdottoman luotettava.

Esillä oleva keksintö kohdistuu menetelmään turvamerkinnän käyttämiseksi. Menetelmässä turvamerkintä liitetään sähköisessä muodossa merkittävään laitteeseen. Merkintä voidaan asentaa laitteeseen tai

esineeseen niin huomaamattomasti, että sen havaitseminen on käytännössä mahdotonta.

Keksinnön mukaisesti turvamerkintä luetaan tunnistuslaitteeseen ja avataan se siihen sisältyvien tietojen saamiseksi. Tietoihin voi kuulua henkilökohtaiset omistajan tunnistetiedot, kuten nimi, sosiaaliturvatunnus ja niin edelleen. Tässä yhteydessä voidaan soveltaa myös esimerkiksi PIN-koodia (PIN, Personal Identity Number), jolloin voidaan muodostaa sähköinen allekirjoitus. Käytettävä PIN-koodi voidaan toteuttaa joko matkaviestimessä tai SIM-kortilla. PIN-koodi ja sen pituus voidaan määritellä sovellukseen sopivaksi, käyttäjä voi myös eräässä sovelluksessa vaihtaa sen niin halutessaan.

Keksinnön eräässä sovelluksessa turvamerkintä muodostetaan siten, että henkilökohtaisista tai muista identifiointitiedoista muodostetaan ensimmäinen merkkijono, joka on ennalta määrätyssä muodossa. Tämä ennalta määrätty muoto voi olla esimerkiksi binäärimuoto, jota on helppo mikroprosessorilla käsitellä. Ensimmäinen merkkijono salataan ensimmäisellä avaimella, jolloin salataan tieto siitä, mitä henkilökohtaisia tietoja turvamerkinnän muodostamisessa on käytetty. Merkkijono allekirjoitetaan sähköisesti. Tämän jälkeen merkkijono salataan merkintälaitteessa esimerkiksi käyttäjän julkisella avaimella salatun merkkijonon muodostamiseksi. Merkintälaitteessa on edullisesti kaksi eri salausavainta.

Merkintälaitteessa olevasta käyttäjän julkisesta avaimesta ei ole laitteen ulkopuolella tietoa. Tällöin identifiointitiedot pysyvät salassa, mikä antaa turvamerkinnän käyttäjälle intimiteettisuojaa. Salattu merkkijono tallennetaan sähköisessä muodossa merkintälaitteeseen, joka on liitetty merkittävään esineeseen tai tuotteeseen.

Turvamerkintä avataan siten, että luetaan salattu merkkijono tunnistuslaitteeseen, joka käsittää

välineet salatun merkkijonon purkamiseksi. Tunnistuslaitteessa on myös purkuavain, johon vain turvamerkinnän omistajalla ja käyttäjällä on käyttöoikeus. Käytännössä käyttöoikeus on purkuavaimen salasana, kuten PIN-koodi, tai muu vastaava koodi, jolla purkuavainta voi käyttää. Käyttäjä voi lähettää tämän purkuavaimen myös sellaisessa salatussa muodossa, että luotettava kolmas osapuoli, esimerkiksi poliisi, voi sen purkaa ja käyttää tätä avainta turvamerkinnän tunnistamiseen.

Edullisesti henkilökohtaisiin tietoihin kuuluu turvamerkinnän omistajan biometrinen näyte. Biometrinen näyte voi olla DNA-koodi, joka on tallennettu turvamerkintään ennalta määrätyssä muodossa. Samaten biometrinen näyte voi olla turvamerkinnän omistajan sormenjälkinäyte, silmänpohjan tai iiriksen kuva. Näistä näytteistä on muodostettu graafinen esitys ja se on koodattu sopivaan muotoon, esimerkiksi binäärimuotoon, jotta se voidaan salata käyttäen jotain tunnettua salausmenetelmää.

Kun henkilökohtaisiin tietoihin kuuluu biometrinen näyte, voidaan kaksinkertaisesti varmistaa se, kenelle turvamerkintä kuuluu. Kun käyttäjä, joka väittää omistavansa turvamerkinnän, antaa salasanan, jolla turvamerkintä voidaan purkaa ja saada käyttäjän henkilötiedot, niin ensimmäinen varmistus on suoritettu, koska purkuavaimen salasana on käyttäjä- ja/tai henkilökohtainen. Tämän jälkeen käyttäjä voidaan liittää turvamerkintään ottamalla hänestä vastaava näyte kuin mitä turvamerkintä sisältää. Jos esimerkiksi turvamerkinnän sisältämä DNA-koodi vastaa käyttäjältä määritettyä DNA-koodia, voidaan olla täysin varmoja siitä, että turvamerkintä kuuluu kyseiselle henkilölle.

Turvamerkintään on liitetty myös omistajan henkilötiedot tunnistusmerkinnän yksilöimiseksi ja omistajan oikeellisuuden saamiseksi.

Keksinnön mukaiseen järjestelmään turvamerkinnän, jota käytetään esineiden ja laitteiden merkitsemiseen liittämällä turvamerkintä sähköisessä muodossa niihin, käyttämiseksi kuuluu tunnistuslaite, johon kuuluu lukulaite tunnistusmerkin lukemiseksi ja prosessorin tunnistusmerkin käsittelemiseksi. Tunnistuslaite voi olla mikä tahansa tunnettu laite, jolla sähköisessä muodossa tallennettu turvamerkintä voidaan lukea. Lisäksi tunnistuslaitteen ominaisuudet määräytyvät pitkälti sen perusteella, miten turvamerkintä on tallennettu. Koska turvamerkintä voidaan tallentaa monessa eri muodossa, kuten graafisessa, viivakoodi-, binääri- tai vastaavassa muodossa, niin voi lukulaitteellakin olla useita ominaisuuksia, vastaavasti.

Keksinnön mukaisesti järjestelmään kuuluu välineet ensimmäisen merkkijonon muodostamiseksi henkilökohtaisista tiedoista ennalta määrätyssä muodossa. Lisäksi järjestelmään kuuluu välineet ensimmäisen merkkijonon salaamiseksi käyttäjän julkisella avaimella salatun merkkijonon muodostamiseksi. Merkkijonon muodostamisvälineet ja merkkijonon salaamisvälineet voivat olla esimerkiksi tietokoneessa tai muussa vastaavassa laitteessa, johon henkilökohtaiset tiedot syötetään ja jolla turvamerkintä muodostetaan. Lisäksi järjestelmään kuuluu merkintälaite salatun merkkijonon tallentamiseksi sähköisessä muodossa. Merkintälaitteeseen syötetään salattu merkkijono ennalta määrätyssä muodossa. Edelleen järjestelmään kuuluu välineet salauksen purkamiseksi tunnistuslaitteessa olevalla purkuavaimella.

Eräässä edullisessa sovelluksessa merkintälaitteeseen kuuluu muistilaite ja ensimmäinen liityntärajapinta merkintälaitteen liittämiseksi lukulaitteeseen. Tunnistuslaite voi olla turvamoduuli, johon kuuluu toinen liityntärajapinta yhteyden muodostamiseksi merkintälaitteeseen. Eräässä edullisessa sovel-

luksessa ensimmäinen ja toinen liityntärajapinta on toteutettu Bluetooth-teknologialla.

Esillä olevan keksinnön etuna tunnettuun tekniikkaan verrattuna on, että keksintö takaa luotettavan ja turvallisen järjestelyn sähköisessä muodossa olevan turvamerkinnän käyttämiseksi. Lisäksi keksintö merkittävästi yksinkertaistaa sähköisessä muodossa olevan turvamerkinnän käyttöä, koska erillistä rekisteröintitietokantaa ei tarvita.

Vielä keksinnön etuna tunnettuun tekniikkaan verrattuna on, että keksinnön ansiosta voidaan turvamerkinnän omistajan oikeellisuus tarkistaa kaksinkertaisesti. Tällöin usein voidaan täysin varmistua siitä, kenelle turvamerkintä kuuluu. Keksinnön mukainen menettely antaa myös turvamerkinnän käyttäjälle intimiteettisuojan, koska tallennetun turvamerkinnän sisällön selvittäminen on hyvin hankalaa riippuen käytettävästä salausalgoritmista.

KUVALUETTELO

Seuraavassa keksintöä selostetaan edullisten sovellusesimerkkien avulla viitaten oheiseen piirustukseen, jossa

kuvio 1 esittää erästä esillä olevan keksinnön mukaista tunnistuslaitetta;

kuvio 2 esittää erästä esillä olevan keksinnön mukaista edullista merkintälaitetta; ja

kuvio 3 esittää vuokaaviota eräästä esillä olevan keksinnön mukaisesta edullista tunnistusmenetelmästä

KEKSINNÖN YKSITYISKOHTAINEN SELOSTUS

Kuviossa 1 on esitetty eräs edullinen tunnistuslaite 1. Tunnistuslaitteeseen kuuluu toinen liityntärajapinta RP2 tunnistuslaitteen yhdistämiseksi merkintälaitteeseen 6. Lisäksi tunnistuslaitteeseen kuu-

luu salaus- ja purkuvälineet 5, 7, joilla salataan merkintälaitteeseen 6 tallennettava informaatio ja puretaan merkintälaitteella luettava salattu informaatio.

Edelleen kuviossa 1 esitettyihin salausvälineisiin kuuluu prosessori 3, joka voidaan suunnitella ja optimoida erityisesti salaustoimintoja varten ja joka salaa, purkaa salauksen ja toteuttaa sähköisen allekirjoituksen, ja muisti 9, joka on yhdistetty prosessoriin sen tarvitsemien avaimien ja parametrien tallentamiseksi. Muistiin 9 voidaan tallentaa turvamoduulin käyttäjän henkilökohtainen purkuavain, käytetyn salausalgoritmin parametrejä ja muita tarpeellisia tietoja. Edullinen esimerkki tässä keksinnössä käytettävästä salausalgoritmista on RSA-menetelmä, mutta myös muita epäsymmetrisiä tai symmetrisiä algoritmeja voidaan sovelluksesta riippuen käyttää.

Tunnistuslaitteen runko 11 on sovitettu vastaamaan matkapuhelimen teholähteen muotoja. Lisäksi runkoon 11 on yhdistetty liitin 12, jolla tunnistuslaite voidaan kytkeä matkapuhelimeen. Liittimen 12 kautta voidaan myös kytkeä teho ja tietoliikenne tunnistuslaitteen ja matkapuhelimen välillä. Tässä sovelluksessa tunnistuslaitteen teholähde vastaa kapasiteetiltaan olennaisesti matkaviestimen teholähdettä ja on siten myös ladattava. Tällöin tunnistuslaite voidaan helposti mekaanisesti ja sähköisesti kiinnittää matkapuhelimeen.

Kuviossa 2 esitettyyn merkintälaitteeseen kuuluu muistilaite 8 ja ensimmäinen liityntärajapinta RP1 merkintälaitteen yhdistämiseksi ulkoiseen laitteeseen, esimerkiksi tunnistuslaitteeseen. Edullisesti merkintälaite 6 voi olla sinänsä tunnettu transpondereitekniikkaan perustuva yleisesti käytetty merkintälaite.

Ensimmäisellä ja toisella liityntärajapinnalla RP1, RP2 tunnistuslaite 1 voidaan yhdistää radio-

teitse tai fyysisesti merkintälaitteeseen 6 niiden välistä tiedonsiirtoa varten. Salattu merkkijono voidaan siirtää merkintälaitteeseen 6 tunnistuslaitteella tai merkintälaitteen valmistuksen yhteydessä. Salattu merkkijono voidaan lukea tunnistuslaitteella tai sitä vastaavalla muulla laitteella, jossa on lukemiseen tarvittavat välineet. Eräs tällainen laite voisi olla turvamoduuli, joka kuvataan patenttijulkaisussa FI 981902. Liityntärajapintojen RP1, RP2 yhteyteen voidaan järjestää niin sanottu Bluetooth -osa, vaikka sitä kuvioissa 1 ja 2 ei esitetäkään. Bluetooth -osalla toteutetaan kyseisen teknologian vaatimat toimenpiteet. Liityntärajapinnat RP1, RP2 voidaan toteuttaa millä tahansa optisella infrapunalinkillä, radiolinkillä tai jollakin tunnetulla väyläliitännällä.

Kuviossa 3 esitetään eräs edullinen keksinnön mukainen tunnistusmenetelmä. Kun merkintälaitteella varustettu esine tai laite halutaan tunnistaa, luetaan tunnistuslaitteella 1 merkintälaitteeseen 6 tallennettu informaatio, lohko 31. Lukeminen voi tapahtua radioteitse tai tunnistuslaite voidaan fyysisesti kiinnittää merkintälaitteeseen. Kun informaatio on luettu tunnistuslaitteelle, annetaan tunnistuslaitteeseen käyttäjän henkilökohtainen salasana, joka mahdollistaa tunnistuslaitteella olevan henkilökohtaisen purkuavaimen käytön, lohko 32. Tämä on ensimmäinen tarkistus tarkistettaessa merkintälaitteen omistajaa. Vain merkintälaitteen omistajalla on merkintälaitteelle tallennetun salatun merkkijonon purkamisessa käytettävän purkuavaimen salasana hallussaan.

Kun käyttäjä on antanut avaimen, tallennuslaitteella 1 puretaan salattu merkkijono, lohko 33. Saadusta puretusta merkkijonosta tarkistetaan henkilön identiteetti ja jos se vastaa henkilön ilmoittamaa identiteettiä, jatketaan lohkoon 35 ja jos ei, voidaan lukuoperaatio ja purkuoperaatio toteuttaa uudelleen, esimerkiksi kolme kertaa, jolloin palataan lohkoon 31.

Lohkossa 35, jos vielä halutaan varmistaa, että henkilö on todella se, joka ilmoittaa olevansa, otetaan henkilöstä biometrinen näyte ja verrataan näytettä merkintälaitteelle tallennettuun näyteinformaatioon. Jos näyte on kunnossa, voidaan olla lähes täysin varmoja henkilön identiteetistä ja siitä, että merkintälaite kuuluu kyseiselle henkilölle. Myös tätä näytteen vertailuprosessia voidaan toistaa esimerkiksi kolme kertaa, jos halutaan varmistua siitä, ettei testin epäonnistuminen ole aiheutunut teknisestä viasta.

Keksintö mahdollistaa paikallisesti tapahtuvan luotettavan tunnistuksen ilman, että tunnistamisen yhteydessä täytyy ottaa yhteyttää erilliseen tietokantaa, josta tunnisteen oikeellisuus tarkistetaan. Erityisesti sähköisen tunnistuksen yleistyessä ajaudutaan helposti tilanteeseen, jossa identiteettiä tarkistetaan useista eri tietokannoista, jolloin myös identiteettisuoja voi kärsiä.

Eräässä esimerkinomaisessa tapauksessa muodostetaan käyttäjän henkilökohtaisista tiedoista ensimmäinen merkkijono. Ensimmäiseen merkkijonoon kuuluu esimerkiksi DNA-koodi ja sormenjälkitieto, jotka on muunnettu digitaaliseen muotoon. Näin muodostettu merkkijono salataan RSA 1024-menetelmällä käyttäen käyttäjän salaista salakirjoitusavainta, jolloin muodostetusta merkkijonosta ei voi päätellä, mistä ruumiinosasta tai osista biometrinen tieto koostuu. Merkkijono allekirjoitetaan sähköisesti ja salataan julkisella avaimella. Näin muodostettu tunniste liitetään salattavaan tuotteeseen.

Turvamerkintä voidaan tarkistaa esimerkiksi matkaviestimeen liitetyllä tunnistuslaitteella, jolloin matkaviestimellä voidaan todistaa käyttäjän oikeus merkittyyn esineeseen tai informaatioon. Sähköinen informaatio voidaan liittää helposti esimerkiksi digitaalisesti tallennettuun tietoon. Esimerkiksi CD-levylle, joka sisältää paljon redundanttista informaa-

tiota, voidaan kätkeä vaikeasti havaittava tunniste, joka löytyy vasta sopivan funktion ulostulona. Informaatioon sekoitettua turvamerkintää ei voi muuttaa, koska se ei näy ulospäin. Turvamerkintä voidaan lukea esimerkiksi jollain tarkistuslukumenetelmällä, jolloin informaation ulostulona saadaan haluttu turvamerkintä. Näin voidaan varmentaa esimerkiksi sähköisen informaation tekijänoikeustietoja, toisin sanoen merkitä sähköinen informaatio jonkin henkilön tai yhteisön nimiin.

Esillä olevaa keksintöä eri rajata edellä esitettyihin esimerkkeihin, vaan monet muunnokset ovat mahdollisia pysyttäessä oheisten patenttivaatimuksien suojapiirissä.

PATENTTIVAATIMUKSET

1. Menetelmä turvamerkinnän tunnistamiseksi, jossa menetelmässä turvamerkintää käytetään esineiden, laitteiden tai informaation merkitsemiseen liittämällä turvamerkintä sähköisessä muodossa niihin, t u n n e t t u siitä, että

luetaan turvamerkintä tunnistuslaitteeseen; ja

avataan turvamerkintä sen sisältämien henkilökohtaisten tietojen saamiseksi.

2. Patenttivaatimuksen 1 mukainen menetelmä, tunnettu siitä, että turvamerkintä muodostetaan siten, että

muodostetaan henkilökohtaisista tiedoista ensimmäinen merkkijono ennalta määrätyssä muodossa;

salataan ensimmäinen merkkijono;

allekirjoitetaan ensimmäinen merkkijono sähköisesti;

salataan allekirjoitettu ensimmäinen merkkijono salatun merkkijonon muodostamiseksi;

tallennetaan salattu merkkijono sähköisessä muodossa merkintälaitteeseen; ja että turvamerkintä avataan siten, että

luetaan salattu merkkijono tunnistuslaitteeseen; ja

puretaan salaus tunnistuslaitteessa olevalla purkuavaimella.

3. Patenttivaatimuksen 1 tai 2 mukainen menetelmä, t u n n e t t u siitä, että henkilökohtaisiin tietoihin kuuluu turvamerkinnän omistajan biometrinen näyte.

4. Jonkin patenttivaatimuksista 1 - 3 mukainen menetelmä, t u n n e t t u siitä, että biometriseen näytteeseen kuuluu turvamerkinnän omistajan DNA-koodi ennalta määrätyssä muodossa.

5. Jonkin patenttivaatimuksista 1 - 3 mukainen menetelmä, t u n n e t t u siitä, että biometriseen

näytteeseen kuuluu turvamerkinnän omistajan sormenjälkinäyte ennalta määrätyssä muodossa.

6. Jonkin patenttivaatimuksista 1 - 3 mukainen menetelmä, t u n n e t t u siitä, että biometriseen näytteeseen kuuluu kuva turvamerkinnän omistajan silmästä ennalta määrätyssä muodossa.

7. Jonkin patenttivaatimuksista 1 - 6 mukainen menetelmä, t u n n e t t u siitä, että biometrinen näyte on binäärimuodossa.

8. Jonkin patenttivaatimuksista 1 - 7 mukainen menetelmä, t u n n e t t u siitä, että liitetään turvamerkintään sen omistajan henkilötiedot turvamerkinnän yksilöimiseksi.

9. Järjestelmä turvamerkinnän, jota käytetään esineiden ja laitteiden merkitsemiseen liittämällä turvamerkintä sähköisessä muodossa niihin, käyttämiseksi, johon järjestelmään kuuluu tunnistuslaite (1), johon kuuluu lukulaite (2) turvamerkinnän lukemiseksi ja prosessori (3) turvamerkinnän käsittelemiseksi, t u n n e t t u siitä, että järjestelmään kuuluu

välineet (4) ensimmäisen merkkijonon muodostamiseksi henkilökohtaisista tiedoista ennalta määrätyssä muodossa;

välineet (5) ensimmäisen merkkijonon salaamiseksi käyttäjän julkisella avaimella salatun merkkijonon muodostamiseksi;

merkintälaite (6) salatun merkkijonon tallentamiseksi sähköisessä muodossa;

välineet (7) salauksen purkamiseksi tunnistuslaitteessa olevalla purkuavaimella.

10. Patenttivaatimuksen 9 mukainen järjestelmä, t u n n e t t u siitä, että merkintälaitteeseen (6) kuuluu muistilaite (8) ja ensimmäinen liitäntärajapinta (RP1) merkintälaitteen liittämiseksi lukulaitteeseen (2).

11. Patenttivaatimuksen 9 tai 10 mukainen järjestelmä, t u n n e t t u siitä, että tunnistuslaite (1) on turvamoduuli.

12. Jonkin edeltävistä patenttivaatimuksista 9 - 11 mukainen järjestelmä, t u n n e t t u siitä, että turvamoduuliin (1) kuuluu toinen liityntärajapinta (RP2) yhteyden muodostamiseksi merkintälaitteeseen.

(57) TIIVISTELMÄ

Esillä olevan keksinnön kohteena on menetelmä ja järjestelmä merkintälaitteen tunnistamiseksi. Keksinnössä käytetään hyväksi informaation salausta ja henkilöstä otettavaa biometristä näytettä. Tämä menetelmä mahdollistaa merkintälaitteen tehokkaan ja luotettavan tunnistamisen. Käytännössä menetelmällä ja järjestelmällä saadaan kaksinkertainen varmistus merkintälaitteen omistajan oikeellisuudesta. Ensin varmistetaan sillä, että omistajan on tiedettävä merkintälaitteelle tallennetun informaation salaukseen käytettävän avaimen salasana ja toiseksi vielä sillä, että henkilöstä otettavan biometrisen näytteen on vastattava merkintälaitteelle tallennettua biometristä näytteen koodia tai siitä muodostettua informaatiota.

(Fig. 1)

PCT/FI99/00851
13-03-2000

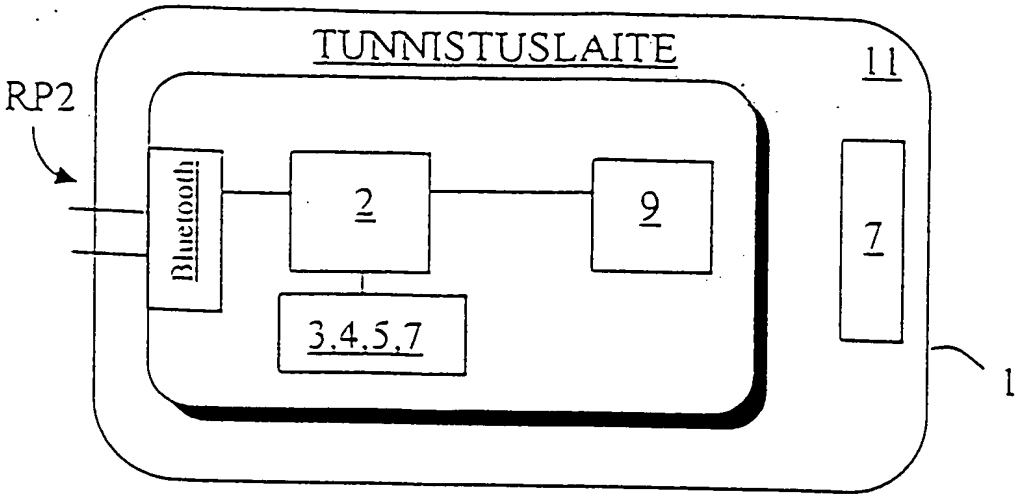

Fig. 1

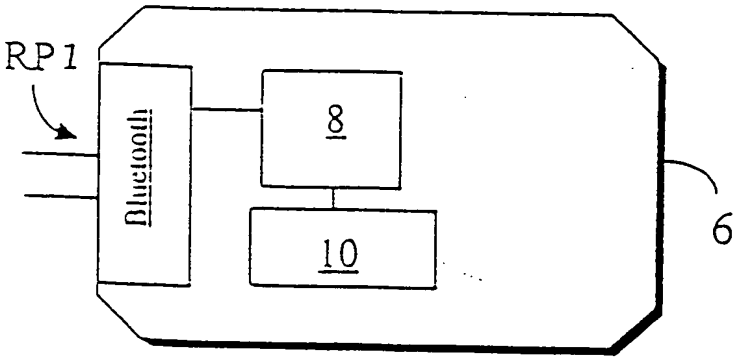

Fig. 2

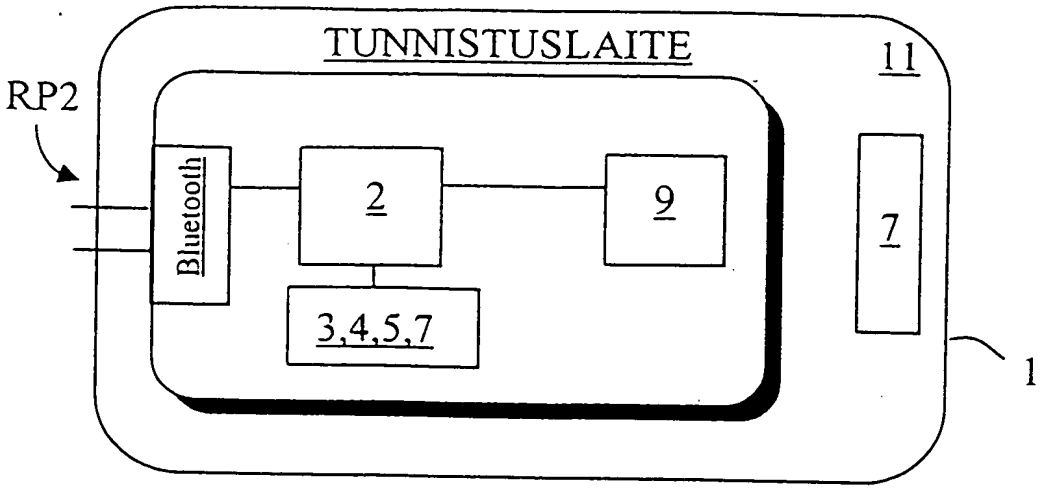
TUNNISTUSLAITE
11
RP2
Bluetooth
2
9
7
3,4,5,7
1

Fig. 1

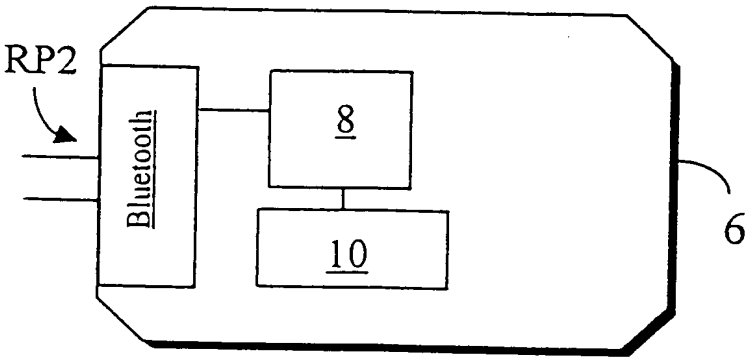
RP2
Bluetooth
8
10
6

Fig. 2

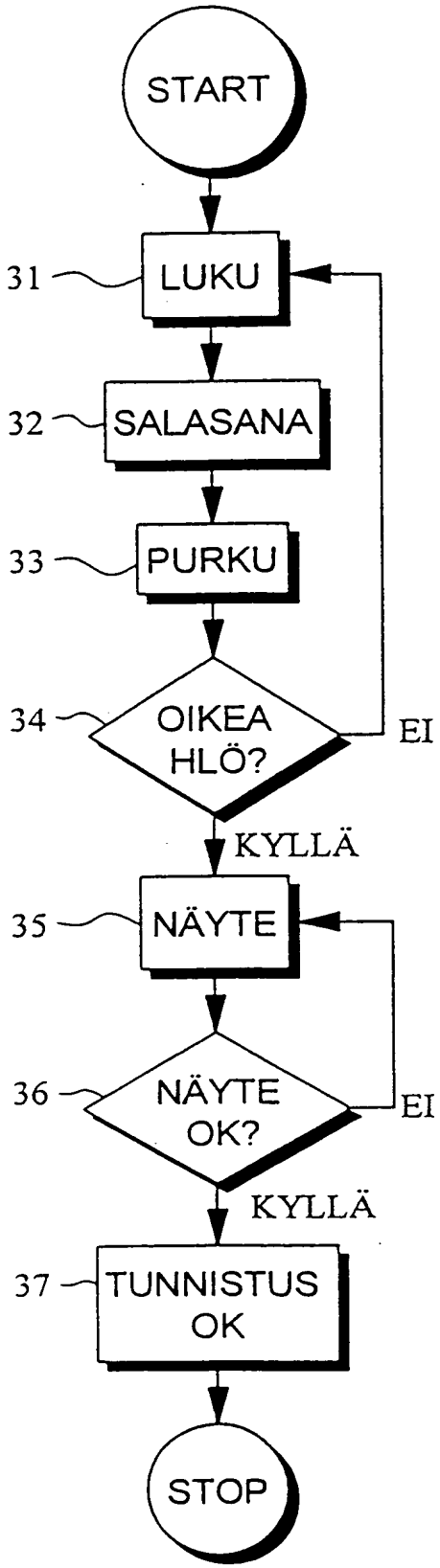
START
31
LUKU
32
SALASANA
33
PURKU
34
OIKEA HLÖ?
EI
KYLLÄ
35
NÄYTE
36
NÄYTE OK?
EI
KYLLÄ
37
TUNNISTUS OK
STOP

Fig 3